Kubernetes Security Testing Report

Date: [Date]

Tester: [Your Name]

Kubernetes Cluster: [Cluster Name]

---

Test Case 1: Kubernetes Dashboard Bypass Authentication (CVE-2018-18264)

Objective: To verify if the Kubernetes Dashboard can be accessed without proper authentication.

Steps:

1. Deploy Kubernetes Dashboard:

- Deploy the Kubernetes Dashboard within the cluster.

2. Access Without Authentication:

- Use OWASP ZAP to send requests to the Dashboard without authentication headers.

- Observe if the Dashboard is accessible without valid credentials.

Results:

The Kubernetes Dashboard should not be accessible without proper authentication. If access is granted without authentication, it indicates a vulnerability that needs to be addressed.

Test Case 2: Cluster-Scoped Custom Resource Access (CVE-2019-11247)

Objective: To validate if the cluster-scoped custom resource can be accessed without appropriate RBAC permissions.

Steps:

1. Create Cluster-Scoped Custom Resource:

- Deploy a cluster-scoped custom resource.

- Use Testkube to validate if the custom resource is accessible without proper RBAC permissions.

Results:

Accessing a cluster-scoped custom resource without the required RBAC permissions could indicate a security vulnerability that allows unauthorized access to sensitive resources.

Test Case 3: kubectl cp Command Tar Exploit (CVE-2019-11249)

Objective: To verify the existence of the kubectl cp command tar exploit.

Steps:

1. Exploit kubectl cp Vulnerability:

- Attempt to exploit the kubectl cp vulnerability using Testkube.

- Check if files can be copied into a pod and if arbitrary code can be executed.

Results:

Successful exploitation of the kubectl cp vulnerability indicates a potential security issue that could lead to unauthorized access and execution of code within pods.

---

Test Case 4: kube-proxy Localhost-Bound Services (CVE-2020-8558)

Objective: To test if kube-proxy makes localhost-bound services accessible from other network nodes.

Steps:

1. Exploit kube-proxy Vulnerability:

- Use Testkube to simulate exploitation of the kube-proxy vulnerability.

- Verify if localhost-bound services are accessible from other network nodes.

Results:

If localhost-bound services are accessible from external network nodes, it indicates a misconfiguration that could lead to unauthorized access to sensitive services.

---

Test Case 5: kube-apiserver Unvalidated Redirect (CVE-2020-8559)

Objective: To test if kube-apiserver is vulnerable to unvalidated redirects.

Steps:

1. Craft Proxied Upgrade Request:

- Use OWASP ZAP to craft a proxied upgrade request with a malicious redirect URL.

- Check if kube-apiserver redirects to the malicious URL without proper validation.

Results:

A successful unvalidated redirect indicates a security vulnerability that can be exploited for phishing attacks or unauthorized access.